3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A14 Benutzung externer Reputation-Services für Apps (H)

Wenn die Administrierenden einer Institution die erlaubten Apps nicht selbst auswählen können und die Benutzenden selbstständig Apps auf ihren Geräten installieren dürfen, SOLLTE ein sogenannter Reputation-Service eingesetzt werden. Das MDM SOLLTE dann mithilfe dieser Informationen aus dem Reputation-Service die Installation von Apps zumindest einschränken.

SYS.3.2.2.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A16 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A17 Kontrolle der Nutzung von mobilen Endgeräten (H)

Es SOLLTEN angemessene Kriterien definiert werden, aufgrund derer die Geräte zu überwachen sind, ohne gegen gesetzliche oder interne Regelungen zu verstoßen. Insbesondere SOLLTEN sogenannte Jailbreaks oder sogenanntes Routen erkannt werden.

SYS.3.2.2.A18 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A19 Einsatz von Geofencing (H)

Durch die Hinterlegung einer Geofencing-Richtlinie SOLLTE sichergestellt werden, dass Geräte mit schutzbedürftigen Informationen nicht außerhalb eines zuvor festgelegten geografischen Bereichs verwendet werden können. Wird der geografische Bereich verlassen, SOLLTEN entsprechend klassifizierte Informationen oder das Gerät vollständig gelöscht werden. Bevor das Gerät selektiv oder vollständig gelöscht wird, SOLLTEN die zuständigen Administrierenden und das Sicherheitsmanagement sowie die Benutzenden informiert werden. Erst mit einer angemessenen zeitlichen Verzögerung SOLLTE das Gerät selektiv oder vollständig gelöscht werden. Die Bereiche, an denen diese zusätzlichen Sicherheitsmaßnahmen nötig sind, SOLLTEN identifiziert werden. Anschließend SOLLTEN die Sicherheitsmaßnahmen unter Beachtung gesetzlicher und interner Regelungen umgesetzt werden.

SYS.3.2.2.A23 Durchsetzung von Compliance-Anforderungen (H)

Verstöße gegen die Regelungen der Institution oder sogar eine Manipulation des Betriebssystems SOLLTEN mit einer geeigneten Lösung erkannt werden. Die folgenden Aktionen SOLLTEN bei Verdacht auf Verstoß gegen Regelungen oder Manipulation des Betriebssystems ausgeführt werden. Hierzu SOLLTEN entsprechende Funktionen bereitgestellt werden:

1. selbstständiges Versenden von Warnhinweisen,
2. selbstständiges Sperren des Geräts,
3. Löschen der vertraulichen Informationen der Institution,
4. Löschen des kompletten Geräts,
5. Verhindern des Zugangs zu Unternehmens-Apps sowie
6. Verhindern des Zugangs zu den Systemen und Informationen der Institution.

Bei Verdacht auf einen Verstoß oder eine Manipulation SOLLTE ein Alarm an die zuständigen Administrierenden und das Sicherheitsmanagement in der Institution gesandt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ das Dokument BSI-CS 052: „Mobile Device Management“ veröffentlicht.

Das BSI hat einen Mindeststandard zum Thema MDM veröffentlicht: „Mindeststandard des BSI für Mobile Device Management nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 11.05.2017“. Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124“, Revision 1, Juni 2013 zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2.3 iOS (for Enterprise)

1. Beschreibung

1.1. Einleitung

Aufgrund von modernen, einfachen Bedienkonzepten sowie ihrer hohen Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit den Betriebssystemen iOS und iPadOS. Da iPadOS auf iOS basiert, werden beide in diesem Baustein zur einfachen Lesbarkeit als „iOS" zusammengefasst. Die beiden Betriebssysteme haben aktuell vor allem funktionale Unterschiede, die den abweichenden Formfaktor der Geräte berücksichtigen.

Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Durch die Umgestaltung der Infrastrukturen und die Art der Informationserhebung und -verarbeitung werden sie jedoch immer häufiger auch im beruflichen Umfeld verwendet und lösen teilweise sogar Notebooks ab.

Durch die Integration von Business-Funktionen wurde iOS seit der Version 4 schrittweise für den Einsatz in Unternehmen und Behörden ausgebaut und Funktionen für die Verwaltung aus Sicht einer Institution integriert. Hierzu gehören die Möglichkeit zur zentralisierten Geräteregistrierung (Apple Business Manager) sowie Optionen wie Single Sign-On (SSO).

1.2. Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit iOS (for Enterprise) betriebene Geräte sicher in Institutionen eingesetzt werden können. Dazu werden Anforderungen für Einstellungen der iOS-basierten Endgeräte aufgestellt, die in Form von Konfigurationsprofilen auf den Endgeräten verteilt werden können. iOS-Konfigurationsprofile enthalten einheitlich definierte Einstellungen, z. B. für Sicherheitsrichtlinien oder einzelne Systemaspekte, um iOS-basierte Geräte einheitlich und zentral zu verwalten und automatisch zu konfigurieren.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.2.3 *iOS (for Enterprise)* ist auf alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Apple iOS anzuwenden.

Dieser Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von iOS-basierten Geräten, die in die Prozesse der Institution integriert sind, zu beachten und zu erfüllen sind. Anforderungen an die Integration in die Sicherheits- oder Kollaborationsinfrastruktur der Institution stehen nicht im Fokus dieses Bausteins. Mit einem sogenannten „Mobile Device Management" (MDM) besteht die Möglichkeit, die Geräte zentral zu verwalten und Konfigurationsprofile pro Gruppe von Benutzenden oder Einsatzzweck auszurollen. Über ein MDM lassen sich auch Sicherheitsmaßnahmen einheitlich umsetzen. Dieser Baustein setzt voraus, dass zu verwaltende iOS-Geräte in eine MDM-Infrastruktur integriert sind. Wird eine geringe Anzahl von Geräten verwaltet, können diese aus wirtschaftlichen Gründen ausnahmsweise ohne MDM eingesetzt werden. Anforderungen für den Betrieb von MDM finden sich im Baustein SYS.3.2.2 *Mobile Device Management (MDM)*. Für kleinere Umgebungen kann der Apple Configurator verwendet werden, um die in diesem Baustein aufgeführten Anforderungen auf mehreren Endgeräten einheitlich umzusetzen. Allgemeine und übergreifende Aspekte zum Betrieb von Smartphones und Tablets, unabhängig vom darauf eingesetzten Betriebssystem, finden sich im Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* und sind ebenfalls umzusetzen, wenn iOS-basierte Geräte verwendet werden.

Für die Nutzung von biometrischen Authentisierungsmechanismen enthält der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* entsprechende Anforderungen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.3 *iOS (for Enterprise)* von besonderer Bedeutung.

2.1. Risikokonzentration durch ein Konto (Apple-ID) für alle Apple-Dienste

Mit der Apple-ID gibt es einen zentralen Zugang zu allen von der Firma Apple zur Verfügung gestellten Diensten (z. B. „iMessage", „FaceTime", „iCloud", „App Store", „iTunes", „iBook-Store", „iPhone-Suche" oder Synchronisationsdienste). Wenn Unbefugte auf eine nicht ausreichend abgesicherte Apple-ID zugreifen können, können sie diese Apple-Dienste unter Umständen nutzen, die Verfügbarkeit der Apple-ID-basierten Dienste stören, iOS-basierte Geräte aus der Ferne lokalisieren oder auf Werkseinstellungen zurücksetzen sowie auf Informationen des Cloud-Dienstes iCloud zugreifen. Insbesondere ist es Angreifenden bei aktivierten iCloud-Backups möglich, die gespeicherten Daten auf ein eigenes iOS-Gerät zu klonen.

2.2. Feste Integration von vorinstallierten Apps und deren Funktionen

Mit iOS liefert Apple bereits fest integrierte und vorinstallierte Apps (z. B. „Mail" und „Safari") aus. Diese Apps werden teilweise mit höheren Berechtigungen als die aus dem App Store herunterladbaren Apps ausgeführt, wodurch sich die Angriffsfläche des iOS-basierten Geräts vergrößert.

2.3. Missbräuchlicher Zugriff auf ausgelagerte Daten

Für eine Reihe iOS-spezifischer Funktionen muss die von der Firma Apple betriebene Infrastruktur verwendet werden. Werden die Funktionen „iCloud-Schlüsselbund", „iMessage", „FaceTime", „Siri", „Continuity", „Spotlight-Vorschläge" sowie Funktionen der iCloud zum Anlegen von Backups oder zum gemeinsamen Arbeiten an Dokumenten verwendet, werden die Daten zwischen unterschiedlichen Geräten oder Benutzenden stets über die Infrastruktur der Firma Apple synchronisiert. Ebenfalls werden Push-Nachrichten für iOS-basierte Geräte über diese Infrastruktur weitergeleitet. Es besteht somit prinzipiell die Gefahr, dass auf Apple-Server zugegriffen wird und die dort gespeicherten oder übertragenen Daten für andere Zwecke missbraucht werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.3 *iOS (for Enterprise)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.2.3.A1 Strategie für die iOS-Nutzung (B)

Wird ein MDM eingesetzt, so MÜSSEN die iOS-basierten Geräte über das MDM verwaltet und konfiguriert werden. Hierzu MUSS eine Strategie zur iOS-Nutzung vorliegen, in der Aspekte wie die Auswahl der Endgeräte oder Strategien für Datensicherungen festgelegt werden. Es MUSS geregelt werden, ob zusätzliche Apps von Drittanbietenden genutzt werden sollen bzw. dürfen. Außerdem MÜSSEN Jailbreaks organisatorisch untersagt und nach Möglichkeit technisch verhindert werden.

SYS.3.2.3.A2 Planung des Einsatzes von Cloud-Diensten (B)

Bevor iOS-basierte Geräte verwendet werden, MUSS festgelegt werden, welche Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen. Dabei SOLLTE berücksichtigt werden, dass iOS-basierte Geräte grundsätzlich eng mit iCloud-Diensten von Apple verzahnt sind. Außerdem SOLLTE berücksichtigt werden, dass beispielsweise bereits die Aktivierung von Einzelgeräten mit einer Apple-ID hiervon betroffen ist. Daher SOLLTE geprüft werden, ob zur Geräteregistrierung Apple Business Manager (früher Device Enrollment Program, DEP) genutzt werden kann.

SYS.3.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A7 Verhinderung des unautorisierten Löschens von Konfigurationsprofilen (B)

Damit Konfigurationsprofile nicht unautorisiert gelöscht werden können, MÜSSEN geeignete technische (z. B. durch den betreuten Modus) oder organisatorische Maßnahmen getroffen und umgesetzt werden. Benutzende von mobilen Endgeräten SOLLTEN für den Sinn und Zweck der Sicherheitsmaßnahmen sensibilisiert werden.

SYS.3.2.3.A8 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.3.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A12 Verwendung von Apple-IDs (S)

Statt einer persönlichen Apple-ID der Benutzenden SOLLTE eine anonymisierte Apple-ID verwendet werden. Falls möglich, SOLLTE der Apple Business Manager für Volumenlizenzen (früher Volume Purchase Program, VPP) sowie eine zentralisierte Installation von Apps verwendet werden.

SYS.3.2.3.A13 Verwendung der Konfigurationsoption „Einschränkungen unter iOS" (S)

Alle nicht benötigten oder erlaubten Funktionen bzw. Dienste von iOS SOLLTEN deaktiviert werden. Basierend auf dem Einsatzzweck und dem zugrundeliegenden Schutzbedarf SOLLTE geprüft werden, welche der Funktionen „Sperrbildschirm", „Unified Communication", „Siri", „Hintergrundbild", „Verbindung mit Host-Systemen" und „Diagnose- und Nutzungsdaten" einzusetzen sind.

SYS.3.2.3.A14 Verwendung der iCloud-Infrastruktur (S)

Bevor die umfängliche oder selektive Nutzung der iCloud-Infrastruktur für eine dienstliche Nutzung freigegeben wird, SOLLTE bewertet werden, ob die allgemeinen Geschäftsbedingungen der Firma Apple mit den internen Richtlinien hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz vereinbar sind. Wird die Nutzung der iCloud-Infrastruktur erlaubt, SOLLTE die Identität am iCloud-Webservice durch eine Zwei-Faktor-Authentisierung geprüft werden. Ansonsten SOLLTE die iCloud-Nutzung für einen rein dienstlichen Bedarf auf ein geringes Maß reduziert oder komplett ausgeschlossen werden.

SYS.3.2.3.A15 Verwendung der Continuity-Funktionen (S)

Wurde die Nutzung der iCloud-Infrastruktur nicht grundsätzlich durch das Sicherheitsmanagement der Institution untersagt, SOLLTE die Vereinbarkeit der Continuity-Funktionen mit den internen Richtlinien unter Berücksichtigung der Aspekte Vertraulichkeit und Integrität bewertet werden. Auf Basis der Bewertungsergebnisse SOLLTE geregelt werden, inwieweit diese Funktionen technisch bzw. organisatorisch eingeschränkt werden.

SYS.3.2.3.A16 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A17 Verwendung der Gerätecode-Historie (S)

Im Konfigurationsprofil SOLLTE die Anzahl der eindeutigen Codes bis zur ersten Wiederholung auf einen angemessenen Wert festgelegt sein.

SYS.3.2.3.A18 Verwendung der Konfigurationsoption für den Browser Safari (S)

Die bereits in der Institution etablierten Browserrichtlinien SOLLTEN entsprechend auch für Safari durch technische und organisatorische Maßnahmen umgesetzt werden. Dabei SOLLTEN die bereits etablierten Anforderungen für Browser auf stationären und tragbaren PCs als Grundlage für die Absicherung der iOS-basierten Geräte dienen sowie die Einsatzszenarien. Das Einsatzumfeld der Geräte SOLLTE beachtet werden.

SYS.3.2.3.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A21 Installation von Apps und Einbindung des Apple App Stores (S)

Um sicherzustellen, dass den autorisierten Benutzenden die benötigten Apps zum notwendigen Zeitpunkt ausreichend zur Verfügung stehen, SOLLTE überlegt werden, den Apple Business Manager in die MDM-Infrastruktur zu integrieren. Zahlungen im App Store SOLLTE NICHT über biometrische Verfahren bestätigt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.2.3.A22 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.3.A23 Verwendung der automatischen Konfigurationsprofillöschung (H)

Geräte, die über einen klar definierten Zeitraum durchgängig offline sind, SOLLTEN ihren Zugang zur internen Infrastruktur verlieren. Nach Ablauf des definierten Zeitraums oder an einem bestimmten Tag, SOLLTE das Konfigurationsprofil ohne Zutun des IT-Betriebs gelöscht werden. Falls Benutzende des Geräts vor Ablauf der Frist auf das interne Netz zugreift, SOLLTE der Zeitraum bis zur automatischen Löschung des Konfigurationsprofils erneuert werden. Falls sicherzustellen ist, ob die Benutzenden noch im Besitz ihres Gerätes sind, SOLLTEN sie aktiv zum Zugriff innerhalb einer Frist aufgefordert werden. Falls die Frist ohne Zugriff verstreicht, sollte das Konfigurationsprofil der entsprechenden Benutzenden automatisch gelöscht werden.

SYS.3.2.3.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.3.A25 Verwendung der Konfigurationsoption für AirPrint (H)

Freigegebene AirPrint-Drucker SOLLTEN den Benutzenden durch ein Konfigurationsprofil bereitgestellt werden. Um zu vermeiden, dass Informationen auf nicht vertrauenswürdigen Druckern von Benutzenden ausgedruckt werden können, SOLLTEN stets alle Kommunikationsverbindungen über die Infrastruktursysteme der Institution geführt werden.

SYS.3.2.3.A26 Keine Verbindung mit Host-Systemen (H)

Um zu vermeiden, dass iOS-basierte Geräte unautorisiert mit anderen IT-Systemen verbunden werden, SOLLTEN die Benutzenden iOS-basierte Geräte ausschließlich mit dem MDM verbinden können.

SYS.3.2.3.A27 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ das Dokument BSI-CS 074: „iOS-Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit“ (Stand 2015) veröffentlicht.

Die Firma Apple stellt im Kontext der Themen dieses Bausteins unter anderem folgende weiterführende Informationen bereit:

- Apple Configurator: https://support.apple.com/de-de/apple-configurator
- Apple Security Updates: https://support.apple.com/en-us/HT1222
- Abgekündigte und Vintage-Produkte: https://support.apple.com/de-de/HT201624
- Apple Business Manager: https://business.apple.com
- Support für Unternehmen und Bildungseinrichtungen: https://www.apple.com/de/support/business-education/

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2.4 Android

1. Beschreibung

1.1. Einleitung

Ein oft genutztes Betriebssystem für Smartphones und Tablets ist Android von Google. Seit Version 4 wurde Android schrittweise für den Unternehmenseinsatz ausgebaut. So wurden z. B. Funktionen integriert, die es Institutionen erleichtern, Android-Geräte zu verwalten. Auch steigt die Zahl der von Android unterstützten Verwaltungsrichtlinien mit jeder Version. Zudem ermöglichen spezifische Erweiterungen der herstellenden Institutionen zusätzliche Richtlinien.

1.2. Zielsetzung

Ziel des Bausteins ist es, über typische Gefährdungen im Zusammenhang mit Android zu informieren sowie aufzuzeigen, wie Android-basierte Geräte sicher in Institutionen eingesetzt werden können. Auf Basis der im Baustein aufgeführten Anforderungen können zudem Sicherheitsrichtlinien erstellt werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.2.4 *Android* ist für alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Google Android anzuwenden.

Der Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von Android-basierten Geräten zu beachten und zu erfüllen sind. Allgemeine und übergreifende Anforderungen an den Betrieb von Smartphones und Tablets werden nicht in diesem Baustein, sondern in SYS.3.2.1 *Allgemeine Smartphones und Tablets* behandelt und sind ebenfalls umzusetzen, wenn Android-basierte Geräte verwendet werden. Ebenfalls nicht Bestandteil dieses Bausteins sind Anforderungen für den Fall einer zentralen Administration von Android-Geräten über ein MDM. Diese sind im Baustein SYS.3.2.2 *Mobile Device Management (MDM)* aufgeführt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.4 *Android* von besonderer Bedeutung.

2.1. Deaktivieren von Sicherheitsfunktionen

Der Bootprozess von Android-basierten Geräten wird mit Hilfe eines Herstellendenzertifikats abgesichert. Dabei wird jeweils der nächste Ausführungsschritt vor dessen Ausführung überprüft. Damit ist sichergestellt, dass das Betriebssystem Android unverändert startet.

Beim Entsperren des Bootloaders wird diese Vertrauenskette unterbrochen, so dass ein verändertes Betriebssystem starten kann. Solche Veränderungen am Bootprozess werden teilweise von der herstellenden Institution unterstützt, teilweise werden Bootloader auch über Schwachstellen entsperrt.

Das Android-Sicherheitskonzept wird hierbei umgangen oder außer Kraft gesetzt und es entstehen neue Gefährdungen, die anderweitig abgesichert werden müssen.

2.2. Schadsoftware für das Android-Betriebssystem

Aufgrund der hohen Verbreitung und der offenen Architektur sind Geräte mit Android-Betriebssystem ein beliebtes Ziel für Schadsoftware, die oft von Benutzenden selbst installiert wird. Unter Android ist es relativ einfach möglich, Apps nicht nur aus dem Playstore von Google, sondern auch aus alternativen Quellen oder per direktem Download zu installieren. Neben den überwachten App Stores von Google, Geräteherstellenden und anderen Anbietenden werden Apps auch über eher zweifelhafte Quellen zur Installation angeboten. Da es unter Android nicht zwingend erforderlich ist, Apps aus dem offiziellen Google Playstore zu installieren, könnten Angreifende beispielsweise eine beliebte App mit einer Schadsoftware infizieren und anschließend wieder zum Download zur Verfügung stellen.

2.3. Fehlende Updates für das Android-Betriebssystem

Einige herstellende Institutionen liefern Smartphones und Tablets mit veralteten Versionen von Android aus oder stellen keine regelmäßigen oder sogar überhaupt keine Updates zur Verfügung. Da regelmäßig Schwachstellen in Android entdeckt werden, sind solche Geräte besonders gefährdet. Als Konsequenz können bekannte Schwachstellen dieser Geräte nicht beseitigt und entsprechend leicht von Angreifenden ausgenutzt werden.

2.4. Risiko durch Konten (Google-ID) für Google-Dienste

Mit der Google-ID können Benutzende zentral auf alle Google-Dienste zugreifen, z. B. auf die Geräteverwaltung, die aufgezeichneten geographischen Positionen, Chatsoftware, Cloud-Speicher, den Play Store, Musik-, Buch- und Filmangebote, Datensicherung, Bookmarks oder Password-Speicher für Webseiten und Synchronisationsdienste. Auch viele andere Anbietende von Diensten im Internet verwenden die Google-ID, um Benutzende zu authentisieren.

Können sich Angreifende über die Google-ID authentisieren, können alle hiermit verbundenen Dienste unter der gestohlenen Identität benutzt werden. Auch können beispielsweise auf alle dort gespeicherten Daten zugegriffen und Geräte aus der Ferne lokalisiert oder zurückgesetzt, also alle Daten auf dem Gerät gelöscht werden.

2.5. Vorinstallierte Apps und integrierte Funktionen bei Android-basierten Geräten

Mit dem Betriebssystem liefern die herstellenden Institutionen von Android-Geräten oft bereits fest integrierte und vorinstallierte Apps sowie eine Anbindung zu Diensten von Drittanbietenden (Twitter, Facebook, usw.) aus. Diese Apps können Benutzende oft nicht selbst entfernen. Damit vergrößert sich die Angriffsfläche des Android-Betriebssystems. Auch die direkte Anbindung an Dienste von Drittanbietenden ist in Institutionen oft nicht erwünscht.

Insgesamt steigt durch die tiefe Integration von Apps und Schnittstellen von Drittanbietenden die Gefahr, dass das Gerät mit Schadsoftware infiziert wird oder Angreifende unberechtigt auf vertrauliche Informationen zugreifen können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.4 *Android* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.2.4.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.4.A2 Deaktivieren des Entwicklermodus (S)

In allen Android-basierten Geräten SOLLTE der Entwicklermodus deaktiviert sein.

SYS.3.2.4.A3 Einsatz des Multi-User- und Gäste-Modus (S)

Es SOLLTE geregelt sein, ob ein Gerät mit anderen Personen geteilt werden darf. Es SOLLTE festgelegt werden, ob dazu der Multi-User- oder Gäste-Modus verwendet werden muss. Benutzende auf einem Android-basierten Gerät SOLLTEN natürliche Personen sein.

SYS.3.2.4.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.4.A5 Erweiterte Sicherheitseinstellungen (S)

Es SOLLTEN nur freigegebene Sicherheits-Apps Rechte zur Geräteadministration bekommen oder sich als „Trust Agents" eintragen lassen. Dies SOLLTE regelmäßig überprüft werden.

Weiterhin SOLLTE es nur erlaubten Apps möglich sein, auf Nutzungsdaten und auf Benachrichtigungen zuzugreifen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.2.4.A6 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.4.A7 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.3.2.4 *Android* gibt es keine weiterführenden Informationen.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.3 Mobiltelefon

1. Beschreibung

1.1. Einleitung

Die in diesem Baustein betrachteten Mobiltelefone, die auch „Feature-Phones" oder „Dumbphones" genannt werden, besitzen weniger Eigenschaften als ein Smartphone, bieten aber mehr Funktionen als nur die reine Telefonfunktion. So können diese Mobiltelefone zusätzlich mit einer Kamera für Videos und Fotos, einem Terminplaner, E-Mail-Programmen, Spielen, einem MP3-Player oder einem Radioempfänger ausgestattet sein. „Klassische" Mobiltelefone verfügen in der Regel nicht über einen Touchscreen und ein Betriebssystem, auf das zusätzliche Apps installiert werden können. Diese fehlenden Funktionen unterscheidet das Mobiltelefon von einem Smartphone.

Mobiltelefone sind durch eine international eindeutige Seriennummer (International Mobile Equipment Identity, IMEI) gekennzeichnet. Die Identifizierung der Benutzenden des Mobiltelefons erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbietenden zugeteilt wird.

1.2. Zielsetzung

Ziel des Bausteins ist es, typische Gefährdungen aufzuzeigen, die bei der Nutzung von Mobiltelefonen auftreten können, sowie Informationen abzusichern, die auf Mobiltelefonen gespeichert sind oder darüber übermittelt werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.3 *Mobiltelefon* ist auf alle Mobiltelefone anzuwenden, die für dienstliche Zwecke verwendet werden.

Dieser Baustein beschäftigt sich mit allgemeinen Aspekten von typischen Mobiltelefonen, mit Sicherheitsaspekten zur Telefonie und Nachrichtenübermittlung über das Mobilfunknetz und mit Sicherheitsaspekten zum Umgang mit den Geräten. Damit deckt dieser Baustein ein großes Spektrum unterschiedlicher Geräte ab, die an Mobilfunknetze angeschlossen werden können. Ergänzende Aspekte, die über die Kommunikation über ein Mobilfunknetz und den Umgang mit den Geräten hinausgehen, sind in weiteren Bausteinen des IT-Grundschutz-Kompendiums zu finden. So können Sicherheitsanforderungen zu Smartphones und den darauf genutzten Betriebssystemen ergänzend den Bausteinen der Schicht SYS.3.2 *Tablet und Smartphone* entnommen werden. Aspekte datenbasierter Telefonie werden im Baustein NET.4.2 *VoIP* behandelt. Verwendet das betrachtete Mobiltelefon VPNs, sollte zusätzlich der Baustein NET.3.3 *VPN* berücksichtigt werden. Für Smartphones oder Tablets ist der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* anzuwenden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.3 *Mobiltelefon* von besonderer Bedeutung.

2.1. Unzureichende Planung bei der Anschaffung von Mobiltelefonen

Werden in der Planungsphase relevante Eigenschaften der anzuschaffenden Mobiltelefone nicht ermittelt, könnten dringend benötigte Funktionen nicht verfügbar sein. Werden bestimmte Mobilfunkstandards nicht unterstützt, können die Geräte in bestimmten Ländern nicht verwendet werden. Im schlimmsten Fall entspricht der Funktions-

umfang nicht dem Einsatzzweck, sodass diese Geräte überhaupt nicht eingesetzt werden können. Oft gibt es auch weitere Randbedingungen, die erfüllt werden müssen, damit die Geräte eingesetzt werden können. Hierzu gehören beispielsweise Sicherheitsfunktionen, die oft nicht auf den ersten Blick ersichtlich sind, aber zu Problemen bezüglich der Verfügbarkeit und Vertraulichkeit führen können, wenn sie verwendet werden.

2.2. Verlust des Mobiltelefons

Da Mobiltelefone in der Regel klein sind und ständig transportiert werden, können sie leicht verloren gehen, vergessen oder gestohlen werden. Neben dem wirtschaftlichen Schaden wiegt der Verlust der Vertraulichkeit und Integrität der enthaltenen Daten besonders schwer. Denn über ein entwendetes Mobiltelefon könnten Angreifende auf institutionskritische Informationen der Institution zugreifen. Außerdem entstehen Kosten und Aufwände, um einen arbeitsfähigen Zustand wiederherzustellen.

2.3. Sorglosigkeit im Umgang mit Informationen bei der Mobiltelefonie

Durch Unachtsamkeit und Sorglosigkeit der Mitarbeitenden bei der Mobiltelefonie können Dritte an schützenswerte Informationen gelangen. So können beispielsweise Informationen bei Telefongesprächen mitgehört oder aufgenommen sowie Nachrichten beim Verfassen mitgelesen werden.

2.4. Unerlaubte private Nutzung des dienstlichen Mobiltelefons

Firmeneigene Mobiltelefone können unerlaubt für private Zwecke verwendet werden. Durch Unachtsamkeit und sorglosen Umgang können so Probleme bezüglich der Informationssicherheit der Institution entstehen, etwa wenn private und dienstliche Inhalte vermischt werden. Auf diese Weise könnten Unbefugte Kenntnis von Interna der Institution erlangen. Werden dienstliche Mobiltelefone privat genutzt, können außerdem zusätzliche Kosten für die Institution entstehen.

2.5. Ausfall des Mobiltelefons

Der Ausfall eines Mobiltelefons kann mehrere Ursachen haben. So können Benutzende versäumt haben, den Akku des Gerätes aufzuladen, oder der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben. Auch ist es möglich, dass Benutzende das Zugangspasswort oder die PIN vergessen haben und das Gerät nicht mehr nutzen können. So kann sich das Gerät bei mehrfach falscher Eingabe des Zugangscodes selbst sperren. Wird mit dem Telefon nicht sorgfältig umgegangen, kann es beschädigt werden, beispielsweise indem es herunterfällt. In allen genannten Fällen sind die Benutzenden anschließend nicht mehr erreichbar und können wiederum selbst niemanden über das Mobiltelefon erreichen.

2.6. Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen

Aufgrund der Eigenschaften von mobiler Kommunikation kann nicht verhindert werden, dass die übertragenen Signale mit entsprechendem Aufwand unbefugt mitgehört und aufgezeichnet werden. Bei den meisten Funkdiensten müssen außerdem die mobilen Kommunikationsgeräte aus technischen Gründen geortet werden, um erreichbar zu sein. Somit können Standort-Informationen durch Netzbetreibende oder Dienstbetreibende verwendet werden, um Bewegungsprofile zu erstellen.

2.7. Abhören von Raumgesprächen über Mobiltelefone

Mobiltelefone können dazu verwendet werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. In Besprechungen können über mitgebrachte Mobiltelefone Verbindungen zu unbefugten Mithörenden aufgebaut werden. Viele Mobiltelefone sind mit einer Freisprecheinrichtung ausgestattet, sodass problemlos Gespräche im gesamten Raum erfasst können. Bei vielen Geräten ist nicht sichtbar, ob sie eingeschaltet sind oder nicht. Somit kann nicht direkt erkannt werden, ob Gespräche aufgezeichnet oder abgehört werden.

2.8. Einsatz veralteter Mobiltelefone

Da Smartphones vielfältiger als Mobiltelefone genutzt werden können, bieten viele herstellende Institutionen inzwischen ausschließlich Smartphones an. Damit übersteigt das Angebot an Smartphones deutlich das Angebot an Mobiltelefonen und es werden kaum noch Mobiltelefone produziert. Aufgrund des geringen Angebots werden zahlreiche Mobiltelefone aus Altbeständen verwendet. Altersschwache Komponenten wie Akkus werden oft durch

Nachbauten von Drittanbietenden ersetzt, sodass diese Mobiltelefone weiterhin Jahrzehnte nach der Produktion eingesetzt werden können.

Oft sind auf diesen veralteten Mobiltelefonen Betriebssysteme installiert, die nicht mehr weiterentwickelt oder supported werden. Softwareschwachstellen können somit nicht mehr durch Updates beseitigt werden. Häufig gibt es die herstellenden Institutionen der Mobiltelefone nicht mehr, oder sie haben ihr Geschäftsfeld auf andere Märkte verlagert. Originales Zubehör und Ersatzteile können deshalb oft nicht mehr nachgekauft werden. Auch Drittherstellende bieten bei sehr alten Mobiltelefonen oft keine entsprechenden Produkte mehr an. Wenn Drittherstellende dennoch Ersatzteile anbieten, ist nicht gewährleistet, dass diese Komponenten die gleiche Qualität wie die originalen Teile besitzen. So sind beispielsweise nachgebaute Akkus oft weniger leistungsfähig als die Originale. In der Regel können diese Geräte auch oft nicht mehr repariert werden und bei Problemen gibt es kaum noch geeignete Ansprechpersonen, die helfen können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.3 *Mobiltelefon* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.3.A1 Sicherheitsrichtlinien und Regelungen für die Nutzung von Mobiltelefonen (B)

Im Hinblick auf die Nutzung und Kontrolle der Geräte MUSS eine Sicherheitsrichtlinie erstellt werden. Jeder benutzenden Person eines Mobiltelefons MUSS ein Exemplar der Sicherheitsrichtlinie ausgehändigt werden. Es MUSS regelmäßig überprüft werden, ob die Sicherheitsrichtlinie eingehalten wird. Die Sicherheitsrichtlinie zur dienstlichen Nutzung von Mobiltelefonen SOLLTE Bestandteil der Schulung zu Sicherheitsmaßnahmen sein.

SYS.3.3.A2 Sperrmaßnahmen bei Verlust eines Mobiltelefons (B) [Benutzende]

Bei Verlust eines Mobiltelefons MUSS die darin verwendete SIM-Karte zeitnah gesperrt werden. Falls möglich, SOLLTEN vorhandene Mechanismen zum Diebstahlschutz, wie Fernlöschung oder -sperrung, genutzt werden. Alle notwendigen Informationen zur Sperrung von SIM-Karte und Mobiltelefon MÜSSEN unmittelbar griffbereit sein.

SYS.3.3.A3 Sensibilisierung und Schulung der Mitarbeitenden im Umgang mit Mobiltelefonen (B)

Mitarbeitende MÜSSEN für die besonderen Gefährdungen der Informationssicherheit durch Mobiltelefone sensibilisiert werden. Sie MÜSSEN in die Sicherheitsfunktion der Mobiltelefone eingewiesen sein. Den Benutzenden MUSS der Prozess bekannt sein, durch den die Mobiltelefone gesperrt werden können. Die Benutzenden MÜSSEN darauf hingewiesen werden, wie die Mobiltelefone sicher und korrekt aufbewahrt werden sollten.

SYS.3.3.A4 Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und darin verwendeter Speicherkarten (B)

Mobiltelefone MÜSSEN vor der Entsorgung auf den Werkszustand zurückgesetzt werden. Es MUSS überprüft werden, ob alle Daten gelöscht wurden. Es SOLLTE zudem sichergestellt werden, dass die Mobiltelefone und eventuell darin verwendete Speicherkarten ordnungsgemäß entsorgt werden. Falls die Mobiltelefone und Speicherkarten erst zu einem späteren Zeitpunkt beziehungsweise in größerer Anzahl entsorgt werden, MÜSSEN die gesammelten Mobiltelefone und Speicherkarten vor unberechtigtem Zugriff geschützt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.3.A5 Nutzung der Sicherheitsmechanismen von Mobiltelefonen (S) [Benutzende]

Die verfügbaren Sicherheitsmechanismen SOLLTEN auf den Mobiltelefonen genutzt und vorkonfiguriert werden. Die SIM-Karte SOLLTE durch eine sichere PIN geschützt werden. Die Super-PIN/PUK SOLLTE nur im Rahmen der definierten Prozesse von den Zuständigen benutzt werden. Das Mobiltelefon SOLLTE durch einen Geräte-Code geschützt werden. Falls möglich, SOLLTE das Gerät an die SIM-Karte gebunden werden (SIM-Lock).

SYS.3.3.A6 Updates von Mobiltelefonen (S) [Benutzende]

Es SOLLTE regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt. Der Umgang mit Updates SOLLTE geregelt werden. Wenn es neue Softwareupdates gibt, SOLLTE festgelegt werden, wie die Benutzenden darüber informiert werden. Es SOLLTE festgelegt werden, ob die Benutzenden die Updates selber installieren dürfen, oder ob die Mobiltelefone an einer zentralen Stelle hierfür abgegeben werden sollen.

SYS.3.3.A7 Beschaffung von Mobiltelefonen (S)

Bevor Mobiltelefone beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste SOLLTEN die am Markt erhältlichen Produkte bewertet werden. Das Produkt SOLLTE danach ausgewählt werden, ob die Herstellenden für den geplanten Einsatzzeitraum Updates anbieten. Es SOLLTE gewährleistet werden, dass Ersatzteile wie Akkus und Ladegeräte in ausreichender Qualität nachbeschafft werden können.

SYS.3.3.A8 Nutzung drahtloser Schnittstellen von Mobiltelefonen (S) [Benutzende]

Drahtlose Schnittstellen von Mobiltelefonen wie IrDA, WLAN oder Bluetooth SOLLTEN deaktiviert werden, solange sie nicht benötigt werden.

SYS.3.3.A10 Sichere Datenübertragung über Mobiltelefone (S) [Benutzende]

Es SOLLTE geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Die dafür erlaubten Schnittstellen SOLLTEN festgelegt werden. Außerdem SOLLTE beschlossen werden, wie die Daten bei Bedarf zu verschlüsseln sind.

SYS.3.3.A11 Ausfallvorsorge bei Mobiltelefonen (S) [Benutzende]

Die auf einem Mobiltelefon gespeicherten Daten SOLLTEN in regelmäßigen Abständen auf einem externen Medium gesichert werden. Muss ein defektes Mobiltelefon repariert werden, SOLLTEN zuvor alle Daten gelöscht und das Gerät auf den Werkszustand zurückgesetzt werden. Es SOLLTEN immer Ersatzgeräte vorhanden sein, um ein ausgefallenes Mobiltelefon kurzfristig ersetzen zu können.

SYS.3.3.A12 Einrichtung eines Mobiltelefon-Pools (S)

Bei häufig wechselnden Benutzenden dienstlicher Mobiltelefone SOLLTE eine Sammelaufbewahrung (Pool) eingerichtet werden. Die Ausgabe und Rücknahme von Mobiltelefonen und Zubehör SOLLTE dokumentiert werden. Vor der Ausgabe SOLLTE sichergestellt werden, dass die Mobiltelefone aufgeladen und mit den nötigen Programmen und Daten für die neuen Besitzenden ausgestattet sind. Zudem SOLLTEN die Benutzenden auf die Einhaltung der Sicherheitsleitlinie hingewiesen werden. Nachdem die Geräte wieder zurückgegeben wurden, SOLLTEN sie auf den Werkszustand zurückgesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.3.A9 Sicherstellung der Energieversorgung von Mobiltelefonen (H) [Benutzende]

Es SOLLTEN angemessene Maßnahmen getroffen werden, um die dauerhafte Energieversorgung von Mobiltelefonen sicherzustellen. Je nach Bedarf SOLLTEN Wechselakkus oder Powerbanks eingesetzt werden.

SYS.3.3.A13 Schutz vor der Erstellung von Bewegungsprofilen bei der Nutzung von Mobilfunk (H) [Benutzende]

Es SOLLTE geklärt werden, ob sich die Erstellung von Bewegungsprofilen durch Dritte negativ auswirken kann oder als Problem angesehen wird. Um eine Ortung über GPS zu verhindern, SOLLTE diese Funktion abgeschaltet werden. Falls eine Ortung über das Mobilfunknetz verhindert werden soll, SOLLTE das Mobiltelefon abgeschaltet und der Akku entfernt werden.

SYS.3.3.A14 Schutz vor Rufnummernermittlung bei der Nutzung von Mobiltelefonen (H) [Benutzende]

Um zu verhindern, dass die verwendeten Rufnummern bestimmten Personen zugeordnet werden können, SOLLTEN Rufnummern für ausgehende Anrufe unterdrückt werden. Außerdem SOLLTEN KEINE SMS- und MMS-Nachrichten versendet werden. Rufnummern von Mobiltelefonen SOLLTEN NICHT veröffentlicht oder an unbefugte Dritte weitergegeben werden.

SYS.3.3.A15 Schutz vor Abhören der Raumgespräche über Mobiltelefone (H)

Damit vertrauliche Informationen nicht abgehört werden können, SOLLTE dafür gesorgt werden, dass keine Mobiltelefone zu vertraulichen Besprechungen und Gesprächen in die entsprechenden Räume mitgenommen werden. Falls erforderlich, SOLLTE das Mitführungsverbot durch Mobilfunk-Detektoren überprüft werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2.1 *Mobile device policy*, Vorgaben für den Einsatz von mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, Dezember 2014“ zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

1. Beschreibung

1.1. Einleitung

Moderne Drucker, Kopierer und Multifunktionsgeräte sind komplexe Geräte, die neben mechanischen Komponenten eigene Betriebssysteme enthalten und Serverdienste und -funktionen bereitstellen. Da die Geräte oft vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur geschützt werden.

Als Multifunktionsgeräte werden Geräte bezeichnet, die mehrere papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren, Scannen sowie auch Versenden und Empfangen von Fax-Dokumenten.

Für viele Geschäftsprozesse und Fachaufgaben wird auch heute noch Papier als Informationsträger benutzt. Damit sind Drucker, Kopierer oder Multifunktionsgeräte wichtige Komponenten in der IT-Infrastruktur. Fallen die Geräte aus oder werden verfälschte Dokumente ausgedruckt, kann sich das mitunter auf kritische Prozesse auswirken und zu erheblichen wirtschaftlichen Schäden führen.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie sich Drucker, Kopierer und Multifunktionsgeräte sicher betreiben lassen, sodass weder Informationen über diese Geräte abfließen können noch durch sie die Sicherheit der übrigen internen IT-Infrastruktur beeinträchtigt wird.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* ist für jeden Drucker, Kopierer oder jedes Multifunktionsgerät im Informationsverbund anzuwenden.

Der Baustein behandelt die Sicherheit von Druckern, Kopierern und Multifunktionsgeräten. Vernetzte oder lokal an IT-Systemen angeschlossene Dokumentenscanner werden nicht explizit berücksichtigt. Die Risiken und Anforderungen lassen sich jedoch aus denen für Multifunktionsgeräte ableiten. Ebenso werden vernetzte Faxgeräte nicht gesondert betrachtet. Die in diesem Baustein aufgeführten Risiken und Anforderungen für die Faxfunktion gelten deshalb auch für diese Art von Geräten. Ergänzend sind die Anforderungen des Bausteins NET.4.3 *Faxgeräte und Faxserver* zu berücksichtigen.

Drucker, Kopierer und Multifunktionsgeräte werden oft an Datennetze angeschlossen. Neben kabelgebundenen Anschlüssen können einige Geräte auch direkt mit einem WLAN verbunden werden. Empfehlungen hierzu sind in den Bausteinen der Teilschicht NET *Netze und Kommunikation* zu finden, wie z. B. im Baustein NET.2.2 *WLAN-Nutzung*.

Auf Druckern, Kopierern und Multifunktionsgeräten sind oft vertrauliche Informationen gespeichert, die nach der Außerbetriebnahme auf den Geräten verbleiben. Geleaste Geräte werden häufig, je nach Vertrag, nach einer vorher festgelegten Nutzungsdauer oder -häufigkeit ausgetauscht. Sie werden spätestens nach Ablauf des Leasingvertrags zurückgegeben. Auch Papier und andere Betriebsmittel können vertrauliche Informationen beinhalten. Bevor diese Geräte und Betriebsmittel ausgesondert, getauscht, instandgesetzt oder zurückgegeben werden, müssen alle sensiblen Informationen von ihnen gelöscht werden. Empfehlungen hierzu sind nicht Gegenstand des vorliegenden Bausteins, sondern sind im Baustein CON.6 *Löschen und Vernichten* zu finden.

Bei Druckservern handelt es sich um IT-Systeme mit Druckwarteschlangen, Druckjobverwaltung und möglichen weiteren Funktionen, z. B. Treiberverteilung oder gesichertes Drucken. Für jeden Druckserver müssen die generellen und betriebssystemspezifischen Sicherheitsanforderungen für Server erfüllt werden. Diese werden nicht in diesem

Baustein, sondern in den Bausteinen SYS.1.1 *Allgemeiner Server* und den jeweiligen betriebssystemspezifischen Server-Bausteinen beschrieben.

Ein essentieller Schwerpunkt bei der Absicherung von Druckern, Kopierern und Multifunktionsgeräten ist es, die auf den Geräten installierte Software regelmäßig zu aktualisieren und dadurch Softwareschwachstellen zu schließen. Der vorliegende Baustein behandelt diesen Aspekt allerdings nicht. Anforderungen hierzu sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* von besonderer Bedeutung.

2.1. Unerlaubte Einsicht in ausgedruckte Dokumente

Ausgedruckte Dokumente verbleiben oft für eine längere Zeit im Ausgabefach von zentralen Druckern und Multifunktionsgeräten, weil beispielsweise erst mehrere Dateien ausgedruckt und später alle zusammen abgeholt werden. Auch kann es sein, dass am Client ein falscher Drucker ausgewählt wurde und sich die Dokumente nicht am erwarteten Ort befinden. Da Etagen- oder Abteilungsdrucker von vielen Benutzenden verwendet werden, können so auch unberechtigte Personen schützenswerte Informationen einsehen oder mitnehmen.

Auch liegengebliebene Ausdrucke in den Ausgabefächern dezentraler Arbeitsplatzdrucker, die sich in unmittelbarer Nähe in den Büroräumen befinden, sind ein Risiko. Denn Personen, die Zutritt zu diesen Räumen haben, könnten die Ausdrucke ebenso einsehen oder entnehmen.

Eine weitere Gefahr sind im Ausgabefach befindliche Faxdokumente und ausgedruckte Sendeprotokolle, auf denen neben Faxnummer, Datum, Uhrzeit und Seitenzahl mitunter ein verkleinertes Abbild der ersten Seite zu sehen ist. Da solche Protokolle erst ausgegeben werden, nachdem ein Fax verschickt wurde oder ein Sendefehler aufgetreten ist, könnten sie auch über einen längeren Zeitraum im Gerät liegen bleiben oder gar nicht abgeholt werden. Dadurch befinden sich unter Umständen vertrauliche Informationen unbeaufsichtigt im Ausgabefach und können im schlimmsten Fall gestohlen werden.

Zudem werden nicht abgeholte Dokumente irgendwann entsorgt. Das geschieht oft, indem die Ausdrucke wahllos in nahegelegene Papierkörbe geworfen werden, statt Ausdrucke mit schützenswerten Informationen sicher zu vernichten. Dadurch können diese Informationen in die öffentliche Müllentsorgung und so in die Hände Dritter gelangen.

Auch viele Telearbeitsplätze werden mit einem eigenen Drucker oder Multifunktionsgerät ausgestattet. Hierdurch können ebenfalls schützenswerte Informationen offengelegt werden.

2.2. Sichtbarkeit von Metadaten

Zusammen mit einem Druckauftrag werden Metadaten gesendet, die in der Regel die Kennung der Benutzenden, Datum, Uhrzeit und den Namen des Druckauftrages enthalten. Diese Daten werden im Bedienfeld und im Webserver vieler Drucker und Multifunktionsgeräte angezeigt. Der Name des Druckauftrages ergibt sich oft aus dem Namen des digitalen Dokumentes. Falls der Drucker über einen integrierten Webserver verfügt, können über einen Browser oft vertrauliche Vorgänge eingesehen werden. Ebenso sind die Metadaten auf den Druckservern im Klartext sichtbar, sofern sie nicht anonymisiert werden. Damit können Dritte an vertrauliche Informationen gelangen. Viele Geräte erlauben es zudem, Druckaufträge abzuspeichern, um sie später nach Authentisierung über eine PIN auszudrucken. Auch in diesem Fall wird der Name aller vorhandenen Dokumente im Bedienfeld eines Ausgabegerätes angezeigt.

Bestimmte Drucker und Kopierer drucken sogenannte „Yellow Dots“ (auch „Machine Identification Code“, „Tracking Dots“, „Secret Dots“) auf das Papier. Diese oft undokumentierten Wasserzeichen können das Datum und die Uhrzeit sowie die Seriennummer des Druckers beinhalten und sind mit dem bloßen Auge kaum zu erkennen. Auf diese Weise kann ein Ausdruck einer Institution oder einer bestimmten Person direkt zugewiesen und so zu der Person zurückverfolgt werden, die den Text verfasst hat. Neben datenschutzrechtlichen Auswirkungen könnten so ungewollt Informationen die Institution verlassen.

Auch Faxprotokolle können bei vielen Multifunktionsgeräten ohne Zugriffsschutz ausgedruckt werden. Selbst wenn nur Telefonnummer, Datum, Uhrzeit und Seitenzahl aufgelistet werden, können damit schon Rückschlüsse auf personenbezogene Daten oder geschäftliche Vorgänge ermöglicht werden.

2.3. Ungenügender Schutz gespeicherter Informationen

Drucker, Kopierer und Multifunktionsgeräte sind oft mit nichtflüchtigen Speichern ausgestattet, auf denen Informationen temporär oder auch längerfristig abgelegt werden. So werden dort z. B. Adressbücher, Dokumente, Fax-Dateien und Druckaufträge abgespeichert. Sind diese Informationen unzureichend geschützt, können Dritte darauf zugreifen und sie auslesen. Unter Umständen können sogar bereits gelöschte Informationen rekonstruiert werden, wenn unsichere Löschmethoden angewendet wurden.

Über Netzprotokolle können Daten im Gerät gespeichert und gelesen werden. Drucker und Multifunktionsgeräte mit Datenträgern sind, wenn diese nicht gesichert werden, oft als nicht autorisierte Fileserver nutzbar. Auf diese Weise können unkontrolliert Informationen dezentral abgespeichert werden, die nicht im Datensicherungskonzept berücksichtigt werden.

2.4. Unverschlüsselte Kommunikation

Druck- und Scandaten werden oft unverschlüsselt über das Netz übertragen. Dadurch können die gesendeten Dokumente mitgelesen werden. Ebenso lassen sich in Druckservern temporär gespeicherte Druckdateien auslesen. Das gilt auch für zentrale Scan- und Dokumentenverarbeitungssysteme.

Weitere Gefahrenquellen sind unverschlüsselte Kommunikationsschnittstellen zur Administration der Geräte. Wird beispielsweise über HTTP, SNMPv2 oder Telnet auf Drucker zugegriffen, werden die Informationen dabei ungeschützt transportiert. Dadurch sind die Zugriffsinformationen inklusive Gerätepasswörter gefährdet.

2.5. Unberechtigter Versand von Informationen

Viele Multifunktionsgeräte können digitalisierte Papierdokumente per E-Mail und Fax verschicken. Ohne besondere Schutzmaßnahmen können dadurch Informationen bewusst oder auch versehentlich an nicht autorisierte Empfänger oder Empfängerinnen gelangen. Benutzende könnten beispielsweise Adressen oder Telefonnummern falsch eingeben. Als Folge werden eventuell schutzbedürftige Daten unbeabsichtigt an falsche Empfänger oder Empfängerinnen gesendet. Außerdem können mithilfe der E-Mail- oder Fax-Funktion vertrauliche Unterlagen schnell nach außen gelangen.

Viele vernetzte Drucker lassen sich so konfigurieren, dass Druckaufträge aus dem Internet per E-Mail empfangen und gescannte Dokumente als E-Mail-Anhang versendet werden können. Dabei lässt sich die freie Eingabe der Absendendenadresse missbrauchen, um E-Mails unter fremden Namen an interne und externe Personen zu versenden.

2.6. Unkontrollierter Datenaustausch über Speicherschnittstellen bei Druckern, Kopierern und Multifunktionsgeräten

Dokumente auf Papier können mithilfe von Multifunktionsgeräten schnell kopiert werden. Durch vorhandene USB- oder SD-Anschlüsse ist es zudem möglich, selbst große Mengen an Papierunterlagen direkt und ohne jegliche Kontrolle zu digitalisieren und auf USB-Sticks oder SD-Karten zu speichern. Auch können über die Speicherschnittstellen hierauf abgelegte Dokumente direkt ausgedruckt werden.

Sind die Drucker, Kopierer und Multifunktionsgeräte an ein Datennetz oder direkt an Clients angeschlossen, können IT-Systeme oft auch direkt auf die an Drucker, Kopierer und Multifunktionsgeräte angeschlossenen Speichermedien zugreifen. Auch wenn die Einbindung von Speichermedien an IT-Systeme selbst technisch verhindert wird, können über diesen Umweg unkontrolliert Informationen über die Speicherschnittstellen kopiert werden.

Auf diese Weise kann zum einen über die Speicherschnittstellen (Schad-)Software über die Multifunktionsgeräte auf den hieran angeschlossen Clients oder in das Datennetz der Institution gelangen. Zum anderen können auch vertrauliche (Papier-)Dokumente unbemerkt digitalisiert und unnachvollziehbar gestohlen werden.

2.7. Ungenügend abgesicherte Netzzugänge von Druckern, Kopierern und Multifunktionsgeräten

Firewalls zwischen LAN und Internet werden häufig so konfiguriert, dass ganze Subnetze auf das Internet zugreifen können. Zudem werden Drucker, Kopierer und Multifunktionsgeräte oft dem gleichen Subnetz zugeordnet wie die Clients. Dadurch können z. B. auch die Netzdrucker auf Informationen im Internet zugreifen. Auch wenn die IT-Systeme der Institution nur über einen Proxy auf das Internet zugreifen, können Drucker, Kopierer und Multifunktionsgeräte diesen ebenfalls nutzen. Wenn die Verbindungen von und zu den Druckern aus dem Internet nicht von der Firewall abgewiesen werden, können unter Umständen schützenswerte Informationen unerwünscht das eigene Datennetz verlassen. Umgekehrt könnte ein netzfähiges Gerät unerwünscht Daten aus dem Internet empfangen und weiter verteilen. Ein Netzdrucker kann dadurch z. B. zu einem Einfallstor für Angriffe aus dem Internet werden.

2.8. Mangelhafter Zugriffsschutz zur Geräteadministration

Vernetzte Drucker, Kopierer und Multifunktionsgeräte können über das Bedienfeld und den eingebauten Webserver verwaltet werden. Bei Auslieferung der Geräte haben diese in der Regel kein oder nur ein Standardpasswort. Wird das Passwort nicht gesetzt oder nicht geändert, kann sehr leicht auf die Geräte zugegriffen werden.

In vielen Institutionen werden zudem einheitliche Passwörter für alle Drucker und Multifunktionsgeräte benutzt, die nur selten geändert werden. Dadurch sind sie oft vielen internen und externen Personen bekannt und unbefugte Dritte können somit einfach auf die Geräte zugreifen.

Weiter lassen sich über Bootmenüs Drucker und Multifunktionsgeräte in den Werkszustand zurücksetzen. Davon betroffen sind auch die Sicherheitseinstellungen. So ist beispielsweise das Gerätepasswort oft nicht mehr vorhanden, nachdem der Drucker oder das Multifunktionsgerät auf die Werkseinstellungen zurückgesetzt wurde. Ungesicherte Bootmenüs erleichtern zwar die Administration, verringern aber gleichzeitig die Sicherheit.

Drucker, Kopierer und Multifunktionsgeräte sind mit zahlreichen Netzprotokollen ausgerüstet. Bei Auslieferung sind meistens alle Protokolle aktiviert. Dadurch könnten Angreifende z. B. auf die Geräteeinstellungen zugreifen und diese so verändern, dass schützenswerte Informationen aus dem Netz abfließen.

Viele Geräte können ihr Bedienfeld über das Netz an den Support übertragen. Damit können jedoch auch vertrauliche Eingaben der Benutzenden am Bedienfeld des Gerätes mitgelesen werden.

In größeren Institutionen gibt es meistens sehr viele Drucker, Kopierer und Multifunktionsgeräte. Um diese noch effizient verwalten und überwachen zu können, wird oft eine Gerätemanagementsoftware eingesetzt. Viele Institutionen schützen diese Software jedoch nicht ausreichend vor unberechtigten Zugriffen, da sie als weniger kritisches System wahrgenommen wird. Dadurch können einzelne oder auch alle Geräte unbeabsichtigt oder bewusst verändert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Informationssicherheitsbeauftragte (ISB)

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)

Bevor Drucker, Kopierer und Multifunktionsgeräte beschafft werden, MUSS der sichere Einsatz geplant werden. Dabei SOLLTEN folgende Kriterien berücksichtigt werden:

- Unterstützung sicherer Protokolle zur Datenübertragung und Administration,
- Verschlüsselung der abgespeicherten Informationen,
- Authentisierung der Benutzenden direkt am Gerät,
- Nutzung physischer Schutzmechanismen, wie Ösen zum Diebstahlschutz oder Geräteschlösser,
- Existenz eines zuverlässigen und leistungsfähigen automatischen Seiteneinzugs der Scaneinheit,
- Unterstützung geeigneter Datenformate,
- Bei Bedarf Unterstützung von Patch- sowie Barcodes zur Dokumententrennung und Übergabe von Metainformationen,
- Existenz einer Funktion zum sicheren Löschen des Speichers sowie
- Verfügbarkeit von regelmäßigen Updates und Wartungsverträgen.

Es MUSS festgelegt werden, wo die Geräte aufgestellt werden dürfen. Außerdem MUSS festgelegt sein, wer auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen darf. Die Ergebnisse SOLLTEN in einem Basiskonzept dokumentiert werden.

SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)

Der IT-Betrieb MUSS Drucker, Kopierer und Multifunktionsgeräte so aufstellen und absichern, dass nur befugte Personen die Geräte verwenden und auf verarbeitete Informationen zugreifen können. Außerdem MUSS sichergestellt sein, dass nur berechtigte Personen die Geräte administrieren, warten und reparieren können. Mit Dienstleistenden (z. B. für die Wartung) MÜSSEN schriftliche Vertraulichkeitsvereinbarungen getroffen werden.

Drucker, Kopierer und Multifunktionsgeräte MÜSSEN mit Gerätepasswörtern versehen sein, um so den Zugriff auf Webserver und Bedienfeld für die Administration zu sperren. Diese MÜSSEN die Vorgaben des Identitäts- und Berechtigungsmanagements der Institution erfüllen.

SYS.4.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A12 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A13 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente (B)

Nicht benötigte, aber ausgedruckte Dokumente mit vertraulichen Informationen MÜSSEN in geeigneter Weise vernichtet werden. Sind Heimarbeitsplätze mit Druckern, Kopierern oder Multifunktionsgeräten ausgestattet, SOLLTE gewährleistet werden, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können, wenn sie nicht mehr benötigt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.1.A4 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten (S)

Die Institution SOLLTE eine Sicherheitsrichtlinie für Drucker, Kopierer und Multifunktionsgeräte entwickeln. Darin SOLLTE geregelt werden, welche Anforderungen und Vorgaben an die Informationssicherheit der Geräte gestellt und wie diese erfüllt werden sollen. Es SOLLTE auch festgelegt werden, welche Funktionen von welchen Benutzenden unter welchen Bedingungen administriert beziehungsweise genutzt werden dürfen.

SYS.4.1.A5 Erstellung von Nutzungsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (S) [Informationssicherheitsbeauftragte (ISB)]

Für die Institution SOLLTE der oder die ISB eine Nutzungsrichtlinie erstellen, auf der alle Sicherheitsvorgaben zum Umgang mit den Geräten übersichtlich und verständlich zusammengefasst sind. Die Nutzungsrichtlinie SOLLTE allen Benutzenden bekannt sein.

SYS.4.1.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (S)

Der IT-Betrieb SOLLTE sicherstellen, dass der administrative Fernzugriff auf Drucker, Kopierer und Multifunktionsgeräte nur einer klar definierten Gruppe des Administrations- und Servicepersonals ermöglicht wird. Das SOLLTE auch dann gewährleistet sein, wenn die Institution eine zentrale Geräteverwaltungssoftware einsetzt.

Es SOLLTE festgelegt werden, ob die Anzeige des Bedienfelds über ein Datennetz eingesehen werden darf. Wenn dies gewünscht ist, SOLLTE es nur an den IT-Betrieb übertragen werden können. Auch SOLLTE dies mit den betroffenen Benutzenden abgestimmt sein.

SYS.4.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (S)

Der IT-Betrieb SOLLTE sicherstellen, dass netzfähige Drucker, Kopierer und Multifunktionsgeräte nicht aus Fremdnetzen erreichbar sind. Wenn Multifunktionsgeräte an das Telefonnetz angeschlossen werden, SOLLTE sichergestellt werden, dass keine unkontrollierten Datenverbindungen zwischen dem Datennetz der Institution und dem Telefonnetz aufgebaut werden können. Netzdrucker und Multifunktionsgeräte SOLLTEN in einem eigenen Netzsegment, das von den Clients und Servern der Institution getrennt ist, betrieben werden.

SYS.4.1.A15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)

Wenn möglich, SOLLTEN alle auf geräteinternen, nichtflüchtigen Speichermedien abgelegten Informationen verschlüsselt werden. Auch Druckaufträge SOLLTEN möglichst verschlüsselt übertragen werden.

SYS.4.1.A17 Schutz von Nutz- und Metadaten (S)

Nutz- und Metadaten wie Druckaufträge und Scandateien SOLLTEN nur so kurz wie möglich auf den Geräten gespeichert werden. Die Daten SOLLTEN nach einer vordefinierten Zeit automatisch gelöscht werden. Dateiserver in den Geräten und Funktionen wie „Scan in den Gerätespeicher" SOLLTEN vom IT-Betrieb abgeschaltet werden. Die dafür benötigten Protokolle und Funktionen SOLLTEN, soweit möglich, gesperrt werden.

Generell SOLLTE vom IT-Betrieb sichergestellt werden, dass alle Metadaten nicht für Unberechtigte sichtbar sind. Es SOLLTE von der Institution geregelt werden, wie mit Metadaten versehene Ausdrucke an Dritte weitergegeben werden.

SYS.4.1.A18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (S)

Alle Drucker und Multifunktionsgeräte SOLLTEN nur vom IT-Betrieb konfiguriert werden können. Nicht benötigte Gerätefunktionen SOLLTEN abgeschaltet werden. Insbesondere SOLLTEN alle nicht benötigten Daten- und Netzschnittstellen von Druckern, Kopierern und Multifunktionsgeräten deaktiviert werden.

Die Geräte SOLLTEN ausschließlich über verschlüsselte Protokolle wie HTTPS und SNMPv3 verwaltet werden. Sämtliche Protokolle, mit denen unverschlüsselt auf Drucker und Multifunktionsgeräte zugegriffen werden kann, SOLLTEN vom IT-Betrieb durch verschlüsselte ersetzt oder abgeschaltet werden. Das SOLLTE insbesondere für Protokolle umgesetzt werden, mit denen sich die Gerätekonfiguration verändern lässt, z. B. SNMP, Telnet und PJL.

SYS.4.1.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (H)

Nur berechtigte Personen SOLLTEN auf die ausgedruckten oder kopierten Dokumente zugreifen können. Es SOLLTEN möglichst nur zentrale Drucker, Kopierer und Multifunktionsgeräte eingesetzt werden, bei denen sich die Benutzenden am Gerät authentisieren, bevor der Druckauftrag startet („Secure-Print"). Nachdem sich die Benutzenden authentisiert haben, SOLLTEN ausschließlich nur die eigenen Druckaufträge sichtbar sein. Nur die für die jeweiligen Benutzenden notwendigen Funktionen SOLLTEN freigeschaltet werden.

SYS.4.1.A16 Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten (H)

Um die Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten so gering wie möglich zu halten, SOLLTEN unter anderem

- Ersatzgeräte bereitstehen,
- in Wartungsverträgen auf eine angemessene Reaktionszeit geachtet werden,
- eine Liste mit Fachhandlungen geführt werden, um schnell Ersatzgeräte oder -teile beschaffen zu können und
- falls erforderlich, häufig benötigte Ersatzteile gelagert werden.

SYS.4.1.A20 Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (H)

Es SOLLTEN auf dem Druckserver die Namen der Druckaufträge nur anonymisiert angezeigt werden. Alle Schnittstellen für externe Speichermedien SOLLTEN gesperrt werden. Weiterhin SOLLTEN geräteinterne Adressbücher deaktiviert und den Benutzenden alternative Adressierungsverfahren (z. B. Adresssuche per LDAP) angeboten werden.

Bei Druckern und Multifunktionsgeräten mit E-Mail-Funktion SOLLTE sichergestellt sein, dass E-Mails ausschließlich mit den E-Mail-Adressen der authentisierten Benutzenden versendet werden können. Auch SOLLTEN Dokumente nur an interne E-Mail-Adressen verschickt werden können.

Eingehende Fax-Dokumente sowie Sendeberichte SOLLTEN nur autorisierten Personen zugänglich sein.

SYS.4.1.A21 Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten (H)

Der IT-Betrieb SOLLTE die Sicherheitseinstellungen von Druckern, Kopierern und Multifunktionsgeräten regelmäßig kontrollieren und, falls notwendig, korrigieren. Wenn ein automatisiertes Kontroll- und Korrektursystem verfügbar ist, SOLLTE es genutzt werden.

Zudem SOLLTE eingeschränkt werden, dass die Geräte über das Bootmenü auf die Werkseinstellungen zurückgestellt werden können. Es SOLLTE sichergestellt sein, dass keine Firmware oder Zusatzsoftware auf Druckern und Multifunktionsgeräten installiert werden kann, die nicht von den jeweiligen Herstellenden verifiziert und freigegeben wurde.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Allianz für Cybersicherheit (ACS) gibt in den BSI-Empfehlungen „Drucker und Multifunktionsgeräte im Netzwerk BSI-CS 015" sowie „Sichere Passwörter in Embedded Devices (BSI-CS 069)" Hinweise zu den genannten Themen. Auch in dem Whitepaper „Datenschutz und IT-Sicherheit in Druckinfrastrukturen" der ACS-Partnerfirma mc^2 management consulting GmbH sind vertiefende Informationen zu Druckern, Kopierern und Multifunktionsgeräten zu finden.

Das National Institute of Standards and Technology (NIST) beschreibt in seiner Special Publication 800-53 „Security and Privacy Controls for Federal Information Systems and Organizations", insbesondere in dem Kapitel „PE-5 Access control for output devices", Anforderungen an Ausgabegeräte wie Drucker, Kopierer und Multifunktionsgeräte.

Das IEEE Standard Schutzprofil für Multifunktionsgeräte im IEEE Std 2600TM-2008 Operational Environment B, „IEEE Std 2600.2TM-2009" wurde von dem IEEE Computer Society, Information Assurance (C/IA) Committee als Basis für die Erstellung von Sicherheitsvorgaben entwickelt, um eine Zertifizierung eines IT-Produkts, des Evaluierungsgegenstands (EVG) durchzuführen.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.3 Eingebettete Systeme

1. Beschreibung

1.1. Einleitung

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind. Sie übernehmen Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben und werden dabei oft nicht direkt von den Benutzenden wahrgenommen. Eingebettete Systeme finden sich sowohl im Bereich der Hochtechnologie wie z. B. der Luft- und Raumfahrt, der Medizintechnik, der Telekommunikation und der Automobiltechnik als auch im Consumer- und Haushaltsgerätebereich.

Ein eingebettetes System bildet aus Soft- und Hardware eine funktionale Einheit, die nur eine definierte Aufgabe erfüllt. Die Software eingebetteter Systeme wird als Firmware bezeichnet und ist zumeist in einem Flash-Speicher, einem EPROM, EEPROM oder ROM gespeichert und durch Anwendende nicht oder nur mit speziellen Mitteln oder Funktionen austauschbar. Sie besteht im Wesentlichen aus dem Bootloader, dem Betriebssystem und der Anwendung. Spezialisierte Systeme können auch auf ein Betriebssystem verzichten. Eingebettete Systeme sind zwar spezialisierte Geräte, aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Als Plattformen kommen unterschiedliche CPU-Architekturen oder flexible hochintegrierte Field-Programmable-Gate-Array-Bausteine (FPGA) infrage.

Eingebettete Systeme haben entweder keine Bedienschnittstelle oder nutzen Spezialperipherie wie z. B. funktionelle Tasten, Drehschalter und auf den jeweiligen Einsatzzweck hin konzipierte Anzeigen. Das Spektrum an Ausgabeeinheiten reicht von einer einfachen Signallampe über LCDs bis hin zu komplexen Cockpit-Anzeigen. Eingebettete Systeme kommunizieren häufig über Datenbusse, die in komplexen Systemen heterogen vernetzt sind. Zusätzlich können über mehrere unterschiedliche und mehrkanalige Ein-/Ausgabeports auch zusätzlich Peripheriekomponenten wie Sensoren und Aktoren angebunden sein. Einige Arten eingebetteter Systeme verfügen darüber hinaus auch über ein Webinterface, über das sie per Browser konfiguriert werden können.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, über typische Gefährdungen für eingebettete Systeme zu informieren sowie aufzuzeigen, wie diese Systeme sicher in Institutionen eingesetzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.3 *Eingebettete Systeme* ist auf jedes eingebettete System im Informationsverbund einmal anzuwenden.

Dieser Baustein beschäftigt sich allgemein mit eingebetteten Systemen. Er ist für ein großes Spektrum unterschiedlicher eingebetteter Systeme anwendbar. Auf dedizierte Sicherheitseigenschaften, etwa von Bedien- und Anzeigesystemen oder spezifische Hard- und Software-Architekturen, wird nicht näher eingegangen. Ebenso wird nicht speziell auf Sicherheitsaspekte von eingebetteten Systemen eingegangen, die in der industriellen Steuerung eingesetzt werden. Hierfür sind zusätzlich die Bausteine der Schicht IND *Industrielle IT* heranzuziehen. Spezifische Sicherheitsaspekte von IoT-Geräten sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Als vernetzte Geräte oder Gegenstände mit zusätzlichen smarten Funktionen werden IoT-Geräte im Gegensatz zu eingebetteten Systemen nicht in ein größeres System oder Produkt integriert. Auf Grund ihrer drahtlosen Verbindung zu Datennetzen bestehen hier andere Sicherheitsanforderungen. Sie werden in SYS.4.4 *Allgemeines IoT-Gerät* behandelt.

Eine besondere Anwendung eines eingebetteten Systems sind Chipkarten. Die Karten besitzen in der Regel einen Prozessor, Arbeitsspeicher und I/O-Interfaces. Auch für Chipkarten gilt, dass zwar grundsätzliche Sicherheitsaspekte in diesem Baustein angesprochen werden, allerdings keine spezifischen Aspekte betrachtet werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.3 *Eingebettete Systeme* von besonderer Bedeutung:

2.1. Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen

Aus Kostengründen spielt die Informationssicherheit bei der Entwicklung von eingebetteten Systemen häufig eine weniger wichtige Rolle als z. B. die Performance oder Zuverlässigkeit. Werden jedoch Sicherheitsanforderungen in einer oder mehreren Entwicklungsphasen nicht ausreichend berücksichtigt, können die eingebetteten Systeme schwerwiegende Schwachstellen aufweisen.

2.2. Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen

Die Schnittstellen eingebetteter Systeme sind potenzielle Angriffspunkte. Das betrifft Schnittstellen auf allen Ebenen des OSI-Schichtenmodells und alle eingesetzten Übertragungsmedien. Wird der Zugang über die Schnittstellen nicht kontrolliert oder sind die Kontrollmechanismen zu schwach, könnte bei einem Angriff in das System eingedrungen werden, unbefugt Daten gelesen und manipuliert sowie Folgeangriffe eingeleitet werden. So könnten unbemerkt Spionage- oder Sabotagegeräte angeschlossen werden, z. B. miniaturisierte Steuerungen oder Datenlogger.

Auf Mikrocontroller-Ebene könnten bei Anschluss der Systeme an die I/O-Ports über die I/O-Leitungen Signale in die I/O-Register eingespielt werden oder es könnten Ausgangssignale aufgezeichnet werden.

Ist ein Reset-Eingang vorhanden, könnten Angreifende diesen ansteuern und temporär das System außer Betrieb setzen.

2.3. Unzureichende physische Absicherung bei eingebetteten Systemen

Sind eingebettete Systeme physisch leicht zugänglich, könnten Angreifende die Systeme zerstören oder beschädigen, z. B. durch mechanische Gewalt, Kurzschlüsse oder Überspannungen. Auch könnten sie auf die elektronischen Komponenten zugreifen, z. B. IC-Pins oder Kontaktierungen, und so die elektrischen Signale mit entsprechenden Mess- und Analysewerkzeugen unbemerkt aufzeichnen sowie selbst Signale einspeisen. Gelangen sie in den Besitz eines eingebetteten Systems, können sie mittels physischer Verfahren Daten lesen und manipulieren oder auf nicht sicher gelöschte Daten zugreifen. Das kann dann dazu führen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der auf dem eingebetteten System gespeicherten Informationen verletzt werden.

2.4. Hardwareausfall und Hardwarefehler bei eingebetteten Systemen

Umgebungseinflüsse wie elektromagnetische Interferenz, Temperaturschwankungen, eine instabile Spannungsversorgung, herstellungsbedingte Materialfehler und Fertigungsstreuung können dazu führen, dass eingebettete Systeme ausfallen. Auch ein normaler oder vorzeitiger Verschleiß, der z. B. durch raue Umgebungseinflüsse wie Staub, Sand oder Verschmutzungen entstehen kann, kann einen Ausfall der Systeme zur Folge haben. Auch könnten hierdurch die umgebenden Systeme stark beeinträchtigen werden.

2.5. Einspielen (Flashen) von manipulierten Software-Updates bei eingebetteten Systemen

Viele eingebettete Systeme speichern ihre Software auf Flash-Speichern und EEPROMs und bieten die Möglichkeit, ihre Firmware mit einem Programmiergerät zu aktualisieren, das über eine Datenschnittstelle oder über eine Netzverbindung angeschlossen wird. Darüber können allerdings auch Angreifende manipulierte Software-Updates einspielen und so die Funktion des Systems modifizieren. In der Folge können die ursprünglichen Aufgaben des Systems unterbrochen oder manipuliert werden.

2.6. Seitenkanalangriffe auf eingebettete Kryptosysteme

Angreifende könnten mittels eines Seitenkanalangriffs Verschlüsselungen oder Signaturen brechen, indem sie dazu beobachtbare Eigenschaften der physischen Implementierung eines Kryptosystems ausnutzen. So könnten sie beispielsweise aus dem Energieverbrauch eines Mikroprozessors während kryptographischer Berechnungen Rückschlüsse auf ausgeführte Operationen und auf Schlüssel ziehen. Auch könnten sie Rechenzeitangriffe, mikroarchi-

tekturelle Angriffe oder (semi-) invasive Angriffe durchführen. So konnten Forschende in der Vergangenheit den geheimen Schlüssel eines TLS/SSL-Servers ermitteln, der den Digital Signature Algorithm (DSA) mit Elliptischer Kurven-Kryptografie verwendet. Der Angriff beruhte auf der Tatsache, dass die benötigte Zeit für eine Multiplikation Rückschlüsse auf deren Operanden zulässt.

2.7. Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen

Eingebettete Systeme sind oft hinsichtlich Codegröße, Zeitverhalten, Energieverbrauch, Kosten sowie Größe und Gewicht eingeschränkt. Sie sind daher häufig nicht mit ausreichenden Sicherheitsfunktionen, wie z. B. starker Kryptografie, ausgestattet. Moderne eingebettete Systeme sind zunehmend durch weitverbreitete Techniken und Protokolle vernetzt und somit potenziell angreifbar.

Bei einem Angriff könnte versucht werden, Daten oder Software auf einem eingebetteten System zu manipulieren, indem versucht wird, die standardmäßig vorgesehenen Kommunikationsschnittstellen und -protokolle für eigene Zwecke zu missbrauchen. Sind z. B. die IP-Kommunikation oder Ethernet-, WLAN-, Bluetooth- und Mobil- oder Digitalfunk-Schnittstellen nicht ausreichend gesichert, können Angreifende Verbindungen übernehmen, Nachrichten fälschen oder in ein System eindringen und Folgeangriffe durchführen. Weiterhin kann ebenso versucht werden, mittels anderer verfügbarer Kommunikationsschnittstellen, z. B. USB-Ports, in das System einzudringen.

2.8. Einsatz gefälschter Komponenten

Im Produktionsprozess oder wenn im Servicefall Komponenten ausgetauscht werden, kann es passieren, dass gefälschte Komponenten in eingebettete Systeme eingebaut werden. Da für viele Bauteile Fälschungen im Umlauf sind, kann dies auch unabsichtlich geschehen. Gefälschte Bauteile arbeiten oft unzuverlässiger als die originalen Bauteile. Hierdurch könnten Funktionen ausfallen oder nur fehlerhaft arbeiten. Angreifende können auch gezielt ein Gerät oder Bauteil entwickeln, das genauso aussieht wie das Original, aber dessen Funktion manipuliert ist. Durch eine derartige Komponente könnten beispielsweise Hintertüren eingebaut, einzelne Funktionen manipuliert oder die Verfügbarkeit eingeschränkt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.3 *Eingebettete Systeme* aufgeführt. Der oder die ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Beschaffungsstelle, Entwickelnde

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.3.A1 Regelungen zum Umgang mit eingebetteten Systemen (B)

Alle Benutzenden und Administrierende MÜSSEN über Verhaltensregeln und Meldewege bei Ausfällen, Fehlfunktionen oder bei Verdacht auf einen Sicherheitsvorfall informiert sein.

Alle eingebetteten Systeme inklusive Schnittstellen MÜSSEN erfasst werden. Die eingebetteten Systeme MÜSSEN sicher vorkonfiguriert werden. Die vorgenommene Konfiguration SOLLTE dokumentiert sein. Weiterhin SOLLTEN Regelungen festgelegt werden, um die Integrität und Funktionsfähigkeit der eingebetteten Systeme zu testen.

SYS.4.3.A2 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen (B)

Es MUSS sichergestellt werden, dass nur auf benötigte Schnittstellen zugegriffen werden kann. Alle anderen Schnittstellen MÜSSEN deaktiviert werden. Zudem DÜRFEN NUR benötigte Dienste aktiviert sein. Der Zugang zu Anwendungsschnittstellen MUSS durch sichere Authentisierung geschützt sein.

SYS.4.3.A3 Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen (B)

Sicherheitsverstöße MÜSSEN protokolliert werden (siehe OPS.1.1.5 *Protokollierung*). Ist eine elektronische Protokollierung nicht oder nur sehr begrenzt realisierbar, SOLLTEN alternative, organisatorische Regelungen geschaffen und umgesetzt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.3.A4 Erstellung von Beschaffungskriterien für eingebettete Systeme (S) [Beschaffungsstelle]

Bevor eingebettete Systeme beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die infrage kommenden Systeme oder Komponenten bewertet werden. Die Anforderungsliste SOLLTE mindestens folgende sicherheitsrelevante Aspekte umfassen:

- Aspekte der materiellen Sicherheit,
- Anforderungen an die Sicherheitseigenschaften der Hardware,
- Anforderungen an die Sicherheitseigenschaften der Software,
- Unterstützung eines Trusted Plattform Module (TPM) durch das Betriebssystem,
- Sicherheitsaspekte der Entwicklungsumgebung sowie
- organisatorische Sicherheitsaspekte.

SYS.4.3.A5 Schutz vor schädigenden Umwelteinflüssen bei eingebetteten Systemen (S) [Entwickelnde, Planende]

Es SOLLTE sichergestellt werden, dass eingebettete Systeme entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts angemessen vor schädigenden Umwelteinflüssen geschützt sind. Die Anforderungen hierfür SOLLTEN bereits bei der Planung analysiert werden. Zudem SOLLTE sichergestellt werden, dass die Vorkehrungen, um einzelne Komponenten vor Staub, Hitze, Nässe und Verschmutzung zu schützen, keine Probleme mit den Anforderungen des übergeordneten Systems verursachen.

SYS.4.3.A6 Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen (S) [Entwickelnde]

Eventuelle Debugging-Möglichkeiten SOLLTEN möglichst vollständig aus eingebetteten Systemen entfernt werden. Wird On-Chip-Debugging genutzt, MUSS sichergestellt werden, dass Debugging-Funktionen nicht unberechtigt genutzt oder aktiviert werden können.

Weiterhin SOLLTE sichergestellt werden, dass keine Eingabeschnittstellen für Testsignale und Messpunkte zum Anschluss von Analysatoren aktiviert und für Unberechtigte nutzbar sind. Zudem SOLLTEN alle Hardware-Debugging-Schnittstellen deaktiviert sein.

SYS.4.3.A7 Hardware-Realisierung von Funktionen eingebetteter Systeme (S) [Entwickelnde, Planende, Beschaffungsstelle]

Werden eingebettete Systeme selbst entwickelt, SOLLTEN bei der Designentscheidung zur Hardware- und Software-Realisierung Sicherheitsaspekte berücksichtigt werden. Auch bei der Entscheidung, eine bestimmte Hardware-Technik zu implementieren, SOLLTEN Sicherheitsaspekte berücksichtigt werden.